ICANN72 | Prep Week – Introducing the DNS Security Facilitation - Technical Study Group (DSFI-TSG)
Thursday, October 14, 2021 – 13:00 to 14:00 PDT

WENDY PROFIT: …to the session introducing the DNS Security Facilitation Technical Study Group. My name is Wendy Profit and I am the remote participation manager for this session.

Please note that the session is being recorded and follows the ICANN Expected Standards of Behavior. During this session, questions or comments will only be read aloud if submitted within the Q&A pod. We will read them aloud during the time set by the chair or moderator of the session.

Interpretation for the session will include all five human languages. Click on the interpretation icon in the Zoom at the bottom of the Zoom tray and select the language you will listen to during the session.

If you wish to speak, please raise your hand in the Zoom Room. This is for the panelists and the session facilitator will call your name. Before speaking, ensure you have selected the language that you will speak from the interpretation menu if speaking any other language than English. And also please state your name for the record and the language that you will speak. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

Please use the drop down menu in the chat pod if you'd like to communicate through the chat, and be sure to select respond to all panelists and attendees. This will allow everyone to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session hosts, the co-hosts, and the other panelists.

To view the real-time transcription, click on the closed caption button in the Zoom toolbar. With that, I will hand the floor over to John Crain.

JOHN CRAIN: Thank you very much, Wendy. Good afternoon, good evening, good morning, everybody. Firstly, I'd like to convey apologies from Göran Marby who had hoped will be able to speak at this but was unfortunately busy with other things, and he asked me to say a few words on his behalf. I'm John Crain. I'm the Chief Security Stability and Resiliency Officer at ICANN and also the interim Chief Technology Officer and have been quite heavily involved in this initiative. As many of you are aware, security, stability and resilience of the identifier systems are core to ICANN's mission, right there front and center in our Bylaws and in everything we do.

Göran approached me in my role about two years ago now after a series of attacks and asked how we could as ICANN better facilitate security in the identifier systems. The process we came up with was to form a Technical Study Group with experts from both within the ICANN community and outside that in the field of security. Göran

received a report from that Technical Study Group earlier this week and it is our intention to have this published on the ICANN website early next week, along with a short-term blog from Göran. I'd like to thank the group on Göran's behalf for this hard work. Volunteers have been working on this series of recommendations for over a year now. I've personally been involved so I watched how hard these volunteers have worked and we cannot thank them enough.

We will take this input as an organization, the impetus to the CEO, and we will study it carefully. And we will come back with a series of ideas of how we can use this information to better facilitate the security of the DNS. With that, I would like to hand it over to Merike Käo who so graciously offered to coordinate these efforts, what was almost a year and a half ago. Merike, over to you, please.

MERIKE KÄO: Yeah. Thank you very much, John. So the session today—this is the agenda for the session—I'll be introducing very briefly the overall work that we've done for the last year and a half. And then we're going to continue into the meat of the work which will discuss attack vectors in the DNS ecosystem, mitigations, and finally, the recommendations, and then leave some time for questions. Each of these sections will have a different member of the TSG speaking. Next slide, please. Next slide.

So as John was mentioning, this work was started in May of last year and it was an initiative that was led and instantiated by the ICANN CEO. It was to execute on his commitment to work with the

community to strengthen the collaboration and communication on the security and stability issues. Primarily, the work was aimed to provide some recommendations on what can and should ICANN be doing to improve the DNS security profile. And also, is there anything that ICANN should specifically not be doing? Next slide, please.

So as John was mentioning, part of this initiative or most of the initiative was really due to some very sophisticated attacks that had been happening quite a few years ago. And we realized or ICANN realized that really the response to some of these sophisticated attacks had been ad hoc. And there needs to be a way to create some more structure on how to respond to these attacks across the Internet ecosystem and to look at where should a new level of collaboration and understanding be necessary. Next slide, please.

So this slide shows the overall timeline of the TSG. The work got started in May and we formulated the TSG membership. The first meeting took place in June 16 of last year. Most of the work in the summer was to define the scope and some key questions that we wanted to address. Then the brunt of the work got started in the early fall and went all the way through to May of this year, where the first part of the discussions were based around root causes and vectors of attack. And then we created a priority list on these particular attack vectors to see which ones were the ones that were more serious and really needed attention to address. We looked at mitigations that existed or that existed but we're not operationalized and also mitigations that may be missing. Then we created the draft document. Once that was finalized and we had some draft recommendations, we

had a technical consultation with some industry experts, and then finally produced the final report and sent it off to Göran earlier this week. Next slide, please.

So this is the membership of the TSG. There's nine members. And as you will see, it's a cross functional group of experts that have in-depth experience and expertise in operating DNS infrastructures in security incident response, general security knowledge, registry/registrar operations, country code registry operations, and also CDN and ISP experience. And also DNS in-depth, DNS technical experience. So the cross functional expertise was rather wide and deep. Next slide, please.

So as I mentioned, also we had a technical consultation review of the draft document, and these are the individuals that submitted very extensive comments. The TSG is extremely grateful for the in-depth review that was provided because it resulted in a much richer final report and recommendations. Next slide, please.

There was also ICANN support in multiple levels. There was a DSFI TSG Steering Committee that consisted of four board members and two executives. We had very extensive support for the work from ICANN for program management, communications, and also technical subject matter expertise. And then bar none, we had an excellent technical writer who, with her skills, turned a very complex intricate topic into a report that you will find when you get access to it is extremely easy to read. Next slide, please.

This slide just shows the breadth and depth of the comprehensive DNS ecosystem. It was expected that the work would take a year, it actually took a year and a half. It was done 100% virtual, which created its own challenges. And I personally want to thank each and every TSG member and the ICANN support staff because we had numerous meetings, also workshops that lasted for two or three hours on a bi-weekly basis to really get to the final result. It's a very complex topic. But again, I am very proud of the final work that we actually came up with. So without further ado, let's get started on discussing the meat of it all and we're going to start with the attack. So next slide, please. Gavin, take it away.

GAVIN BROWN: Certainly, yeah. Thank you, Merike. So this section of the presentation is going to be talking about some of the attack vectors we looked at, and also looking at the methodology we used when looking to analyze them. So if you'd move on to the next slide, please.

This slide is intended to illustrate—in a similar sense to the slide that Merike just showed—the depth and breadth or scope of the systems that we were looking at in terms of the threats and the attack vectors against them. So we're covering—you will see both the DNS side and also on the provisioning side. So this diagram shows both the elements that exist in the DNS resolution path from stub resolvers through to authority servers but also on the provisioning side as well. So that includes end users as registrants, the systems that they interact with to provision domain names, the protocols between

registries and registrars and also intermediaries like resellers. So the intention was to cover the entirety of these different systems and look at all the different attack vectors that could threaten those systems. Next slide, please.

So the process that we went through, very similar to in my experience to almost like a risk analysis in that we looked at the different possible attack vectors and tried to categorize them and come up with commonalities between them. So we talked about each of those specific attack vectors and drew them out from incidents that we had real world experience from. And then when we looked at each attack vector, we looked at a number of different questions around what mitigations might be available—we'll talk about mitigations a bit later on—where the gaps might be, whether issues around incomplete understanding of risks, and whether the DNS infrastructure, the DNS system itself was uniquely vulnerable to particular kinds of issues that other parts of the Internet ecosystem didn't have. Next slide.

So at a high level, we came up with a fairly large number of attack vectors that we condensed down into the ones that you'll see here. They're pretty broad and you'll see that some of them are very kind of generic because the participants in the DNS ecosystem, they're organizations, they're companies just like any other, and they have the same security challenges as every other company, whether you're a bank or a car wash or a gTLD operator. Some of them are unique to the DNS and also unique to the protocols and systems that the participants in the system use. So you'll see that we cover things like the choice of TTLs on records, but also just basic stuff like how good

are your password policies and so on. These were then further condensed into the vectors that are described on the next slide. We can move on please.

So these got condensed down into these categories of attack vectors. Again, we'll talk about some of these in a bit more detail, starting with the ones that are quite generic in general. So identity and access management is a security challenge that is not unique to our world. Every company that has a computer somewhere has to think about this. Same with access control and authorization. There are some areas where that are specific to the DNS system. However, things like resource impersonation, the issues around Denial of Service and also issues around vulnerabilities, both in implementation in code but also in the protocols themselves. And the choices that we've made when we're building infrastructure that cause systems to be vulnerable that you might not expect to move on. Can we move on to the next slide, please?

Starting with the first, identity and access management, credentials exist all over the place in the infrastructure and the provisioning system, and also in the authoritative system as well. They're used to authenticate the interactions between the participants. So if you were an employee of registry, then you'll use a username or password to log into the administration system about registry. If you're a registrar, you'll use a username and password to access the EPP system of the registry. If you're an employee of the registrar, then you're accessing their systems using your username and password, and so on and so forth, all the way through down to the end user. Any point in that

system, those credentials are subject to compromise. And the organizations that are involved in managing those credentials have to make decisions around implementing policies to protect them against the sorts of attacks you would expect to see—password spraying, password reuse, phishing, so on and so forth. So that was the focus of our work in this area, focusing particularly on the credentials of registrants, the authentication between registries, registrars, and resellers, and the threat of using compromised credentials to initiate transactions with the registry by impersonating one of the entities in the chain between the registrant and the registry. Next slide, please.

So here is an example of inadequate access control authorization issue. This is really in relation to subdomain takeover. So this is a scenario where a record exists inside a domain name that has an alias or CNAME record that points to some other resource. This allows a situation where an attacker can essentially take control of that domain name without much validation that they are really the person that owns the domain. Next slide, please.

The next attack vector is in relates to resource impersonation. This is a way in which an attacker can cause DNS queries to be redirected to a third party. This direction can have a number of different implications depending on where it happens in the system. So this can be done sometimes as part of legitimate use. So captive portals—quite a common place where DNS traffic that's intended to exit a network is intercepted by that network in order to present the user with a login form for the captive portal. But it can also be the result of malicious activity, for example, by installing malware on the computer or the

end users device by active interception on the network. So some of the ways in which that could be implemented through impersonation of a recursive resolver, by impersonation of the authority server that's the recursive servers is sitting in between the end user and the source of the authority zone data.

Look-alike domains or facsimile domains. This is somewhat different to you might say—this isn't just phishing but it is somewhat different in that it's the targets in this situation are users of infrastructure rather than end users of consumer services. Fraudulent issued certificates and root manipulation also considered as part of this attack vector. Moving on to the next slide.

This is an example of what we're talking about with a facsimile domain. Homographic attacks are the most obvious example of this form of attack vector.

Next attack vector we talked about was vulnerabilities in code and protocol. There are different issues and challenges we're dealing with these two different kinds of vulnerabilities when there is an issue with DNS software. That is generally the way that that's mitigated is obviously quite different to the way protocol vulnerability is mitigated. Because when there is an issue with the DNS protocol, as we've seen, not most recently, but with a number of vulnerabilities around things like SADDNS, and of course, the most famous, the Kaminski attack. Changing your protocol has interoperability implications. If you change your protocol without careful coordination with all the different operators and implementers, then you have the risk of

destabilizing the system. But they do need to be addressed and they can have a negative impact on systems that are vulnerable. And as you can see, things like cache poisoning are particularly relevant in the case of protocol vulnerabilities. Next slide.

This is an example of how cache poisoning works. As you'll see—I think we've missed the arrows out. Are they visible? Here we go. So they're visible on the next slide.

So where a recursive server receives a query from an end user, so they're looking for icann.org and an active attacker is able to intercept that query or send a fraudulent spoof response back to the recursive server before the answer from the authoritative server is able to be received by the recursive server that ends up with the spoofed answer being sent to the end user before the legitimate response is received by the recursive server from the correct authoritative server. Move on to the next slide.

Infrastructure choices. These are decisions made by the operator of a DNS system or DNS service that can have unintended consequences in terms of the security and availability of that system. TTLs are good example of this. And obviously, we've listed both long TTLs and short TTLs as issues here. So it's really about the Goldilocks TTL of not being too short, not being too long, but being just right in the middle. There are scenarios where short TTL is useful and appropriate. And there are scenarios where a long TTL is useful and appropriate. But the unintended consequences do mean that you need to make a careful risk assessment for making sure that the consequences of those

decisions don't come back and bite you in the bottom. So if we can move on to the next slide to just illustrate that.

So this is a scenario where a TTL has been implemented on a record on an authoritative server. That TTL ensures that the end users will continue to receive queries or answers to queries within the space of that TTL since the cached record will be provided by the resolver. But if the attacker is able to intercept the query either by hijacking the domain name or by one of the other vectors that we've talked about in this section, then the malicious answer would be cached for that period and the users would still be vulnerable to being exploited through that TTL until the record expires and the correct answer can be retrieved from the authoritative server. Next slide.

So we talked about DNS as an attack vector itself. This primarily isn't around things like data exfiltration and use of DNS as a covert channel. DNS is often allowed to transit and exit from a network without being filtered or being blocked, and that is being exploited in a number of different ways to allow attackers to either infiltrate a system or exfiltrate data from that system to the outside. Next slide, please.

Finally, we talked about Denial of Service. This is for any operator of critical DNS infrastructure is a continuous and overriding challenge and problem. Because of the way that the DNS protocol works, the use of UDP means that DNS services are vulnerable to spoofing attacks, they're vulnerable to amplification and reflection attacks. Denial of Service attacks on DNS providers can disrupt the work of significantly

more organizations then would be the case if that target is the operator of root servers of registry or registrar service than simply an end user being subject to Denial of Service attack. Next slide, please.

That concludes our overview of the attack vectors. I'll pass over to one of my colleagues to talk about the mitigations. Duane?

DUANE WESSELS: Hi, everyone. This is Duane Wessels and I'm going to go through the mitigation section of this presentation and our report. Next slide, please.

As Gavin talked about some of the attacks already, we also spend time in the group talking about ways that these attacks can be mitigated, and we came up with a lot of different things. Some of them did not actually make it into the final report but I'm here to talk about the ones that did make it into the report. Next slide.

We spent a lot of time in the group talking about authentication and a lot of the recommendations and mitigations you'll see are around access controls and authentication. So one of the best things that people can do to keep DNS resources safe is to use complex passwords. There are a number of cases where overly simple passwords have led to compromise. Similar to complex passwords, folks could use one-time use credentials or multi-factor authentication. And of course, as our credentials and passwords get more complex, it almost becomes necessary to use some kind of

password manager where that is the thing that remembers your passwords for you rather than trying to remember them yourself.

We talked about risk awareness, which really refers to being aware of the different ways that credentials can become compromised, for example, with phishing attacks. We talked about the availability and use of services that can prevent weak passwords. So for example, there might be some code out there that can tell you whether or not a certain password is strong enough or has certain strength requirements. There are also databases of known compromised passwords that you can check. It's always a good idea to assume that the bad guys have access to these databases as well. So you don't want to use passwords that have already been compromised elsewhere.

We talked about what are some of the remedial solutions that that can take place in case of an attack. Lastly, we talked about ways that domains and registrants can be verified and validated for potential customers when they submit service requests. Next slide, please.

Mitigations in terms of availability, integrity, and privacy. Some of these are already pretty well known, I would say. For availability, I think a lot of people know that single points of failure are a really bad idea. And often, we think about this in terms of networks and network services. Don't put all of your DNS servers on the same network or in the same data center, for example. But there are of course, other types of single points of failure that you might think of such as only using one type of software or even one type of hardware, and so on. Also, as

was made clear to a lot of people in the well-known Dyn attack, if you're using secondary DNS services, it's usually a good idea to spread that among different platforms. Because, again, if you have a single platform and that provider goes down, then you may be out of luck.

In terms of integrity, one of the best mitigations of course is DNSSEC to have signed domains and to implement DNSSEC both on the publication side and on the resolution side to implement validation. Registry lock and some of those similar products are really good ideas to prevent domain hijacking, if those are available to you. Then we also talked about the use of some newer protocols such as the CDS, CDNSKEY, and CSYNC protocols that make it easier basically to transmit DNSSEC material between a child zone and a parent zone.

In terms of privacy, obviously, there's been a lot of work recently about the use of encrypted DNS transport. We're starting to see more and more of that and that's a really good way to implement privacy for DNS. Next, please.

Some other mitigations that people should definitely be aware of are monitoring. You can subscribe to brand protection services. That would, for example, alert you if your company's brand trademark and domain name is registered in another registry or top-level domain. That's probably something you might want to know about. Certificate transparency is a project that makes SSL certificate requests available for people to see. There are services out there that will alert you if there has been a certificate issued for your domain. And if you didn't

issue that yourself, then that's something you probably want to know about.

There's a Certification Authority Authorization records, CAA record that you can put into your zone which specifies which certificate authorities are allowed to issue certificates for your domain. That's a good idea to look into that.

In terms of routing RPKI and route origin, authentication announcements are something that can help protect your networks from false advertisements. You can monitor those as well.

For organizations that need to implement any kind of inspection of the data that's passed to the network, they probably need to consider routers or switches that are optimized for deep packet inspection and can peek into those packets and inform the people about what's passing through the network.

For software developers, we talked about the need to have good software development lifecycle practices. That's just a standard approach to software development that brings in best current practices for keeping software up to date, patched and tested. And of course, I'm sure everyone knows that it's important to patch software regularly, not only from a user point of view but also from the point of view of developers, to keep patches up to date and fix problems as they're found. Next, please.

Mitigations related to access control include the use of what we call behavior-based access architectures. For example, zero trust is one of

these. It's been getting a lot of attention recently. It's always a good idea to partition critical services. For example, separate your DNS services from your e-mail services, from your web services into different systems so that if one is attacked, it doesn't affect the other. Consider, of course, more restrictive access controls for accounts that may be more sensitive.

In cases especially where you are able to partition services, it's a good idea to restrict access for data services to only the DNS ports. That's Port 53, Port 853 now with TLS, and maybe Port 443 with DNS over HTTPS. And if you operate a DNS resolver, that is not really designed to be used by third parties, make sure that it has appropriate access controls that limits its use to only the users who should be using it. Next, please.

Indications for endpoint and network controls. Antivirus is something that has been around for a long time and is still relevant for a lot of users. We didn't spend a lot of time talking about antivirus in the report but there was a brief mention of it there. Strict control over DNS resolver selection means that these days a lot of devices receive from the network, from a DHCP server, for example, the TCP server tells them which resolver to use. That generally works but there are also ways that malware or other vectors of attack can change the recursive name server that a device has been given to something else. Network operators want to pay attention to that. Either perhaps block non-authorized DNS resolvers on a firewall or perform other checks to make sure that the DNS resolver that device is using are correct and appropriate. Of course, again, for organizations that are in a position

to protect their users, something like a DNS firewall is a good idea to really make sure that those users are going to only appropriate and safe destinations. Next, please.

About the mitigations that we talked about in the report, they were divided into these categories which I have mostly covered already. Some of these are, again, credential challenges, access controls for user accounts, and so on. Resource impersonation is something that Gavin talked about, as well as code and protocol vulnerabilities. The report talks about use of DNS as the attack vector versus DNS as the target. Denial of Service attacks, of course, and incident response mechanisms. I believe that's my last slide. And then we hand it over to Marc.

MARC ROGERS: Hello. My mic won't come on. Okay. Next slide. I'm going to talk about the recommendations that came out of the discussions we had in the group. There's an obvious tie back to the attack vectors that were discussed, and the mitigations that were discussed. They broadly fall into these five areas: operational improvements, research, contracting, funding, and education and awareness. Next slide.

The first recommendation that came out is that ICANN should work with other organizations like SSAC, GNSO, ccNSO, TLD Ops to prepare a program for tabletop exercises. Through this program should work to create opportunities to exercise operational functions during incident-like situations to identify operational gaps that might appear. By continually doing this, these operational gaps can be identified,

recorded, and tracked by ICANN and other bodies so that they can then be worked on and flagged in future recommendations. Next slide.

Several research recommendations came out of this. The first one is around DNS Abuse. The threat landscape is never static. It's constantly evolving and so is DNS abuse. The abuse techniques of yesterday evolve and become new techniques tomorrow. And also new avenues open up as different technologies get deployed or as different DNS architectures get deployed. So our recommendation was that we should continually drive research into DNS abuse to make sure that we're always understanding what is the current form of abuse and where is abuse going so that we can get ahead of it.

Next recommendation is that we should investigate which recommendation was that DNS security enhancements should be investigated. And likewise, because the threat landscape is constantly changing, so are DNS security enhancements. Again, we believe there should be a program developed that investigates the limits, risks, and benefits of various DNS security enhancements. A number of those enhancements are listed below in the report. But the overall thinking is like with abuse, we need to keep on top of this, we need to keep monitoring it, and need to create a feedback cycle where gaps are identified, improvements are identified, and these are constantly fed back.

Tying into the conversations about authentication in previous sections, we believe that there should be an investigation into appropriate best practice for authentication. I think the ICANN, along

with other relevant organizations communities, should conduct a study and offer report on what should be considered to be the best practice for authentication when considered against the different roles and risks that face DNS. Next slide.

In contracts and funding, the contract recommendation was that ICANN should work to empower contracted parties to adopt security enhancements to domain registration systems and authoritative name services as practical. We believe by doing this, we can ensure and empower organizations to implement much stronger DNS security.

The next one is focused around bug bounty programs. This was a lively topic for the group because there are a lot of perspectives around where bug bounties fit in, how effective they are, and how they should be adopted. What we all agreed on, though, was that ICANN should lead work into the feasibility of doing bug bounty programs for DNS. Because there are a number of areas where, for example, DNS infrastructure is not owned by a specific organization or DNS infrastructure is no longer being maintained, where it would be advantage to have a managed bug bounty program to focus on those areas and focus on those pieces of software to identify vulnerabilities. Now, because this is such a challenging topic, we believe that the best approach is to make a feasibility study into this to look at the best approach, to look at the most cost effective approach, and to look at how the vulnerabilities from this can be siphoned to the right entities to ensure that they actually are addressed. Next slide.

We believe that there's a very strong need for education and awareness. We think that ICANN should work to build and communicate educational programs that encourage DNS stakeholders to make appropriate standards based authentication mechanisms for all interactions that should be authenticated. As well as informing those stakeholders with a risk associated with weak authentication schemes, that there is way too much legacy authentication that is being leveraged out of simple ignorance. And we believe there is a strong opportunity through education and awareness to move towards much stronger authentication schemes.

Registry lock. ICANN should undertake efforts to improve documentation and understanding of registry lock features and promote their uses when appropriate, also to improve the understanding regarding the differences between registry and registrar lock. Registrants should be able to find clear definitions of what these features provide, what these features do not provide, and what the differences are between them. ICANN should also consider facilitating the standardization of minimum requirements for registry and registrar lock services. Next slide.

We believe that there's a need to drive awareness for best practice in terms of infrastructure security. ICANN needs to work with initiatives like manner and kindness to measure and report on their adoption and their use of reports to target educational material that will improve awareness around infrastructure security. ICANN should take the best practices coming out of those initiatives and make sure that contracted parties and the ICANN community are aware of them.

Where best practices do not exist, ICANN should work to encourage the development and deployment of these practices and promote adoption of DNS security announcing features throughout the DNS ecosystem. For example, DMARC, SPF, TLSA, DANE, DNSSEC, etc.

Next, recommendations around DNS blocking and filtering. ICANN should create informative and educational materials to help the ICANN community, contracted parties and other interested parties to understand the risks and benefits of DNS blocking and filtering for security and stability reasons throughout the global DNS community. Next slide.

With regards to incident response, ICANN should, together with all relevant parties, encourage the development and deployment of a formalized incident response process across the DNS industry that allows for interaction with others in the ecosystem. Such an effort would include incident response handling as well as protected sharing of threat and incident information. And this again can tie back into the tabletop exercise to ensure that any such incident response plans can be enacted in any gaps in operational functionality to do that can be identified.

Recommendation E6, it was covert channel awareness. ICANN should publish educational material on the use of covert channels as an attack vector, which may be seen as abuse of the DNS itself and as such requires handling with other DNS abuse issues. Next slide.

In terms of the top two priorities that we could select out of the recommendations are made, we feel that first is Recommendation R3,

investigate appropriate best practice for authentication. And second is Recommendation E5, incident response. Next slide.

Okay. Off to you, Merike.

MERIKE KÄO: Great. Thank you very much. For anybody that wants to have more information about the Technical Study Group and basically the view what the charter was, the scoping document, the work plan timelines, meeting agendas and notes, and other resources, please go to the site. And as John mentioned, the report will be made public sometime next week along with a blog. I will just warn you ahead of time, it has a lot of content in more detail than we were able to present here in this short amount of time. But a lot of really good content and I think you will find it very valuable. I certainly hope that the ICANN CEO will find this a valuable report that then will get acted upon. At this point in time, I'd like to open it up for any questions that still remain. I don't see any questions in the pod at this point in time.

WENDY PROFIT: I believe all the questions in the pod have been answered in writing.

MERIKE KÄO: Yes, they have been. I'm wondering if there's any new questions, please do write them into the Q&A pod, we'd be happy to address them. Okay. There's the question again, "Where can I get the final report?" The final report will be made available next week along with

the blog. I believe that the pointer will also be in the wiki site that I just pointed to. The question was, "Are these Q&As provided with the recording?" I will leave that up to staff. Is there going to be a transcript along with the recording?

WENDY PROFIT: Let me check with the MTS team on that.

MERIKE KÄO: Okay. Thank you very much. Thank you for the question, Donna. As you can tell, I mean, there was a lot of time in the last 18 months put into this work and the cross functional expertise is bar none, really. It was excellent. I want to thank each and every member that contributed to this report.

At this point in time, I don't see any other questions. If that's the case, I want to thank everybody who participated in this preparatory session. Again, please do have a read of the report when it will be available next week and look forward to see what happens with it.

WENDY PROFIT: We do have one more question in the pod while we're waiting for the other answer, which is, "What are the main motivations of attackers? And where are countries of origin?"

MERIKE KÄO: I'll take this one. But anybody else from the TSG can also contribute. The motivations are just varied. It can be just individuals still, there's also organized crime, and really, it can come from any nation state. That is just the nature of the virtual world that we live in today. All right, with that, I will end this session. Thank you very much, everybody, for attending.

[END OF TRANSCRIPTION]